공개특허 제2001-43378호(2001.05.25) 1부.

[첨부그림 1]

(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(51) Int. Cl.[7]
H04Q 7/38

(11) 공개번호 특2001-0043378
(43) 공개일자 2001년05월25일

(21) 출원번호 10-2000-7012397
(22) 출원일자 2000년11월06일
번역문제출일자 2000년11월06일
(86) 국제출원번호 PCT/US1999/08913 (87) 국제공개번호 WO 1999/57843
(86) 국제출원출원일자 1999년04월23일 (87) 국제공개일자 1999년11월11일
(81) 지정국 AP ARIPO특허 : 가나 감비아 케냐 레소토 말라위 수단 시에라리온 스와질랜드 우간다 짐바브웨

EA 유라시아특허 : 아르메니아 아제르바이잔 벨라루스 키르기즈 카자흐스탄 몰도바 러시아 타지키스탄 투르크메니스탄

EP 유럽특허 : 오스트리아 벨기에 스위스 사이프러스 독일 덴마크 스페인 핀랜드 프랑스 영국 그리스 아일랜드 이탈리아 룩셈부르크 모나코 네덜란드 포르투칼 스웨덴

OA OAPI특허 : 부르키나파소 베넹 중앙아프리카 콩고 코트디브와르 카메룬 가봉 기네 기네비쏘 말리 모리타니 니제르 세네갈 차드 토고

국내특허 : 아랍에미리트 알바니아 아르메니아 오스트리아 오스트레일리아 아제르바이잔 보스니아-헤르체고비나 바베이도스 불가리아 브라질 벨라루스 캐나다 스위스 중국 쿠바 체코 독일 덴마크 에스토니아 스페인 핀랜드 영국 그레나다 그루지야 가나 감비아 크로아티아 헝가리 인도네시아 이스라엘 인도 아이슬란드 일본 케냐 키르기즈 북한 대한민국 카자흐스탄 세인트루시아 스리랑카 라이베리아 레소토 리투아니아 룩셈부르크 라트비아 몰도바 마다가스카르 마케도니아 몽고 말라위 멕시코 노르웨이 뉴질랜드 폴란드 포르투칼 루마니아 러시아 수단 스웨덴 싱가포르 슬로베니아 슬로바키아 시에라리온 타지키스탄 투르크메니스탄 터어키 트리니다드토바고 우크라이나 우간다 미국 우즈베키스탄 베트남 유고슬라비아 짐바브웨

(30) 우선권주장 09/074,475 1998년05월07일 미국(US)
(71) 출원인 인텔 코오퍼레이션 피터 엔. 데트킨
미합중국 캘리포니아 산타클라라 미션 칼리지 블러바드 2200
(72) 발명자 라슨로버트아.
미국캘리포니아95682신굴스프링스다이아우드드라이브5267
헤이즌피터케이.
미국캘리포니아95603오번히든오크스레인2450
굴리아니샌딥케이
미국캘리포니아95630폴솜펌버리웨이109
하스번로버트엔.
미국캘리포니아95667플레이스빌모타라코트2460
탈레자산제이에스.
미국캘리포니아95630폴솜박스카웨이105
웅콜린
미국캘리포니아95831새크라멘도문크레스드웨이7448
브라운할스더블유.
미국캘리포니아95630폴솜하퍼레인123
켄달데리엘.
미국캘리포니아95619디아아몬드스프링스피.오.박스1194
(74) 대리인 특허법인 신성 박해천, 특허법인 신성 원석희, 특허법인 신성 정지원

심사청구 : 없음

(54) 셀룰러 전화의 부정 사용을 방지하기 위한 방법 및 장치

18-1

[첨부그림 2]

요약

전자 시스템(100)의 사용을 제어하기 위한 방법 및 장치가 기술된다. 상기 전자 시스템(100)의 사용은 적어도 하나의 고유 코드를 상기 전자 시스템(100)의 보조 메모리(112) 안에 프로그래밍함으로써 제어된다. 상기 보조 메모리(112)는 상기 메인 메모리(110) 어레이 공간의 외부에 위치하는 영구적 로크가능 메모리이다. 상기 고유 코드는 적어도 하나의 소자 코드와 비교된다. 상기 전자 시스템(100)의 사용은 상기 고유 코드와 상기 소자 코드 사이에 사전 정의된 관계를 바탕으로 제어된다.

대표도

도1

색인어

이동 통신, 셀룰러 전화, 해적 행위, 부정 복제, SIM 카드

명세서

기술분야

본 발명은 셀룰러 전화의 부정 사용을 방지하는 것에 관한 것으로, 특히 부정 방지를 위한 고유한 식별 구조에 관한 것이다.

배경기술

무선 통신은 오늘날 사회에 많은 영향을 끼치고 있다. 불과 몇 년동안, 셀룰러 전화는 미국, 유럽 및 아시아에서 수백만의 가입자를 가지게 되었다. 이러한 극적인 발전은 원격 통신 혁명의 시작이기도 하지만, 이것은 또한 셀룰러 전화의 침해 행위(piracy) 및 부정적인(fraudulent) 사용에서의 혁명의 시작이기도 하다.

통상적인 종래 셀룰러 전화는 데이터, 코드, 또는 양쪽 모두를 저장하기 위하여 비휘발성 기록가능 메모리(nonvolatile writeable memory)를 사용한다. 이러한 비휘발성 기록가능 메모리는 EEPROM(Electrically Erasable Programmable Read-Only Memory) 및 플래시 EPROM(Flash Erasable Programmable Read-Only Memory)을 포함한다. 통상적인 종래 셀룰러 전화의 플래시 메모리는 장치 일련 번호(Equipment Serial Number: 이하, "ESN"이라 칭함) 또는 국제적 이동 장치 식별자(international Mobile Equipment Identifier: 이하, "IMEI"이라 칭함)를 포함한다. 셀룰러 전화가 동작될 때, 셀룰러 서비스 제공자(cellular service provider)가 유저(user)에게 셀룰러 네트워크에 대한 액세스를 제공하고, 그 유저에게 네트워크 접속에 대한 요금을 청구할 수 있도록, 해당 유저가 합법적인 가입자인지를 식별하기 위하여 상기 ESN 또는 IMEI이 브로드캐스팅(broadcasting)된다. 셀룰러 전화 서비스의 요금 지불을 피하기 위하여, ESN 또는 IMEI를 부정적인 수단으로 획득하여 다른 셀룰러 전화 안에 재프로그래밍하면, 부정 복제(fraudulent cloning)가 발생한다. 그리고, 내장형 시스템(embedded system)이 유사한 문제에 직면함에 따라, 그 제품을 역으로 처리하기 위해 플래시메모리로부터 애플리케이션 코드(application code)가 판독된다.

해적 행위(piracy) 또는 부정 행위(fraud)는, 전형적인 아날로그 셀룰러 전화에서, 셀룰러 전화로부터 전송된 아날로그 신호가 인터셉트(intercept) 및 디코딩되어 셀룰러 침해자(cellular pirate)에게 브로드캐스팅한 유저의 ESN 또는 IMEI를 제공된 경우에 발생한다. 그리고 나서, 셀룰러 침해자는 획득한 ESN 또는 IMEI를 이용하여, 이를 다른 아날로그 셀룰러 전화 안에 프로그래밍한다. 이 부정하게 복제된 셀룰러 전화가 사용된 경우, 그 접속시간(airtime)은 침해된 ESN 또는 IMEI에 대해 요금이 청구된다.

셀룰러 해적 행위에 대한 다른 기회는, 셀룰러 전화 하드웨어가 외국의 서비스 제공자에 의해 지원된 경우에 발생한다. 예를 들어, 영국에서의 서비스 제공자는 셀룰러 전화를 가입자에게 2년 서비스 청약의 경우 200달러의 비용으로 제공할 수 있다. 반면, 핀란드에서의 서비스 제공자는 2개월 서비스 청약의 경우 1000달러의 비용으로 셀룰러 전화를 가입자에게 제공할 수 있다. 따라서, 셀룰러 전화는 그것이 사용되는 국가에 따라서 현저히 다른 가치를 가진다. 셀룰러 침해자가 영국에서 200달러의 비용으로 셀룰러 전화를 구매하여, 이를 핀란드에 가져가 1000달러 이하지만 200달러의 구매가격보다는 훨씬 비싼 값으로 팔 수 있는 부정한 기회가 발생한다.

표준 하드웨어 보안 보호 구조가 없기 때문에, 각 OEM(Original Equipment Manufacturer)은 각자의 부정 방지 구조를 구현해야만 한다. 셀룰러 전화의 일부 OEM은 셀룰러 해적 행위를 방지하기 위한 노력을 하지 않는다. 통상적인 종래 셀룰러 전화에서 일부 OEM에 의해 사용되는 부정 방지 기술의 하나는 셀룰러 전화 시스템의 소프트웨어 메모리 공간에 특별한 코드를 심어두는 것이다. 시스템 소프트웨어는 코드의 주소를 알고 있고, 이 코드를 시스템 소프트웨어에 액세스하는데 사용한다. 이 기술이 가진 문제점은 전체 메모리 및 신규 설치 시스템 소프트웨어를 제거하고, 본래 그 장소의 동일한 ID(IDentification)를 재프로그래밍함으로써 쉽게 정복된다는 것이다.

통상적인 종래 GSM(Grobal System for Mobile commnication) 셀룰러 전화에서의 다른 문제점은 가입자 식별 모듈(Subscriber Identification Module:이하, "SIM"이라 칭함) 카드 또는 스마트 카드(smart card)의 부정 사용에 있다. 신용카드 크기인 SIM 카드는, 유저가 해외에 있는 동안 발신 또는 수신을 허가하고, 그들이 집으로 돌아왔을 때 요금이 청구되도록 셀룰러 전화 안에 삽입된다. 상기 SIM 카드가 GSM 셀룰러

18-2

[첨부그림 3]

전화에서의 사용을 위해 설계되는 동안, 카드-작동 공중 지불 전화(card-operated public pay phones)와 같은 비GSM(non-GSM) 전화에서 상기 SIM 카드를 사용하도록 하는 연구가 있어왔다. 그러나, SIM 카드가 부정한 남용을 방지하기가 매우 어렵다는 사실 때문에, 이것의 유용성에 대한 제한을 증가시키지 못하고 있다.

GSM 스마트 카드는 유저가 그들이 가입한 것 외의 다른 GSM 네트워크에서 통화를 하기 위해 필요한 정보를 실어나른다. 이것은 특히 해외를 여행하는 동안 유용하며, 이론상으로 유저가 유럽 전체 및 보다 확대하여 유럽의 밖에서도 역시 아무런 문제없이 발신 또는 수신을 할 수 있도록 한다. 그러나, 그것을 다루는 네트워크 오퍼레이터(operator)의 부정 행위 및 명백한 무능은 오퍼레이터와 이동 전화 유저를 사이의 중간에서의 그룹인 서비스 제공자의 많은 증가가 GSM SIM 카드의 유용성을 고의적으로 제한한다는 것을 의미하고 있다. 이러한 스마트 카드의 초기 목적을 사실상 제거하는 제한은 그것이 제공된 전화에서만 SIM 카드가 동작하도록 제한하는 것을 포함한다. 또한, 셀룰러 전화 해적행위의 결과로, 일부 서비스 제공자는 SIM 카드 전체를 제거하며, 범죄자가 사용할 수 있는 새로운 레벨의 복잡성을 제시하는 것이 논의되고 있다.

외국 서비스 네트워크 오퍼레이터에 의해 초래된 실질적인 손실의 결과, 현재 다수의 외국에서의 많은 외국 서비스는 해외에 있는 동안 사용할 수 있도록 하는 GSM SIM 카드를 이제 디스에이블한다. 지금부터는 해외에 있는 동안 그들의 전화를 사용하길 원하는 경우, 많은 예치금을 남겨 네트워크에 대한 가입자는 이들 서비스 제공자를 통해 남겨둘 것이다. 또한, 현재 일부 외국 사업자는 모든 국제적 로밍을 중지하고 있다.

발명의 상세한 설명

발명의 요약

전자 시스템 사용을 제어하기 위한 방법 및 장치가 기술된다. 전자 시스템의 사용은 상기 전자 시스템의 보조 메모리 안에 적어도 하나의 고유 코드(unique code)를 프로그래밍함으로써 제어된다. 상기 보조 메모리는 메인 메모리 공간의 외부에 위치하는 영구적 로크가능 메모리(permanently lockable memory)이다. 상기 고유 코드는 적어도 하나의 소자 코드(component code)와 비교된다. 이 전자 시스템의 사용은 상기 고유 코드와 소자 코드 사이에 사전 정의된 관계를 바탕으로 제어된다.

본 발명의 다른 특징 및 장점은 첨부된 도면과 이하의 상세한 설명 및 첨부된 청구항으로부터 명확해 질 것이다.

도면의 간단한 설명

도1은 부정 방지 회로의 일실시예를 포함하는 전자 시스템을 도시한 도면.

도2는 플래시 메모리 장치의 일실시예를 도시한 블록도.

도3은 OTP 레지스터 또는 보호 레지스터의 일실시예의 메모리맵을 도시한 도면.

도4는 보호 레지스터의 일실시예에 대해 허용가능한 워드-와이드 어드레싱(word-wide addressing)을 도시한 도면.

도5는 보호 레지스터의 일실시예에 대해 허용가능한 바이트-와이드 어드레싱(byte-wide addressing)를 도시한 도면.

도6은 플래시 메모리 장치의 일실시예의 읽기 구성 테이블(Read Configuration table)을 도시한 도면.

도7은 전자 시스템 제어 방법의 일실시예를 도시한 순서도.

도8은 부정 방지 방법의 일실시예를 도시한 순서도.

실시예

전자 시스템의 사용 및 액세스를 제어하기 위한 방법 및 장치가 기술된다. 특히, 셀룰러 전화의 부정 사용을 방지하기 위한 방법 및 장치가 기술되며, 여기서, 식별 코드는 전자 응용제품 안에서 판독은 되지만 수정은 되지 않도록 하는 메모리 장치를 위한 특별한 식별 구조가 제공된다. 일실시예에서, 셀룰러 전화 OEM은 메모리 장치 제조자에 의해 영구적 로크가능 메모리 또는 원타임 프로그램가능(OTP: One-Time Programmable) 메모리 공간에 고유의 식별 코드 또는 번호가 제공된다. 대안의 실시예에서, 셀룰러 전화 OEM은 플래시 메모리의 OTP 메모리 공간 안에 고유 식별(ID) 코드를 설정한다. 상기 OTP 메모리 안의 식별 코드는 두 실시예 모두에서 수정이 불가능하다.

두 실시예의 동작에서, 셀룰러 전화 시스템 소프트웨어는, 셀룰러 전화를 사용하여 전화 통화가 이루어지도록 허가하기 전에, 상기 OTP 메모리 공간의 고유 식별 코드와 다른 소자 코드 사이의 부합(match)를 체크한다. 상기 부정 방지 회로의 의도된 장점은 셀룰러 전화의 부정한 복제 방지 및 셀룰러 접속 시간 및 전화 보조금의 약탈을 방지하는 것을 포함할 수 있다. 또한, 의도된 장점은 전자 시스템의 액세스 방지, 훔친 컴퓨터 사용 방지, 컴퓨터의 불법적인 또는 인증되지 않은 사용의 방지 및 이러한 시스템으로부터 판독되어지는 애플리케이션 코드를 방지함으로써 전자 시스템 설계의 보안을 강화시키는 것을 포함한다. 또한, 상기 일실시예의 메모리 장치의 고유 식별 코드는 종래 셀룰러 전화의 부정 복제 방지 기술을 향상시킬 수 있도록 사용될 수 있다.

여기서 이미 토의된 바와 같이, 셀룰러 전화의 부정 복제는 하나의 셀룰러 서비스 제공자의 셀룰러 전화가 다른 셀룰러 서비스 제공자에 의해서도 작동되도록 수정되는 경우에 발생한다. 통상적으로, 이것은 셀룰러 전화의 메모리를 제거 및 교체 또는 소거 및 재프로그래밍함으로써 이루어지는데, 이것은 메모리는 특정 셀룰러 서비스 제공자에 대해 효과가 있는 셀룰러 전화 소프트웨어를 포함하기 때문이다. 셀룰러 전

18-3

[첨부그림 4]

화의 불법 복제는 셀룰러 전화 메모리, 셀룰러 전화 하드웨어 및 셀룰러 전화의 마이크로 콘트롤러를 함께 연결 또는 링크함으로써 방지할 수 있다. 이 링크는 특정 셀룰러 전화의 하드웨어를 특정 서비스 제공자에 대해 로킹(locking)함으로써 불법 복제를 방지한다. 따라서, 여기서 기술되고 청구된 방법 및 장치는, OEM 및 서비스 제공자가 실제 전화를 추적하고, 이로부터 데이터베이스를 셋업(setup)하도록 함으로써, 증대의 해적 행위에 대한 해결책을 제공하는데, 이것은 유저 또는 부정 거래자가 ESN, IMEI 또는 그 외의 전자 식별 코드를 수정하는 것을 방지한다.

상기 부정 방지 장치의 일실시예는 플래시 메모리 장치 안에 고유 식별자 코드를 구비하는 두 기회를 제공한다. 셀룰러 전화 OEM은, 셀룰러 전화의 플래시 메모리, 상기 플래시 메모리 안에 내재된 플래시 메모리 코드 및 마이크로 콘트롤러 또는 중앙 프로세서 간의 핸드셰이킹(handshaking)에서, 셀룰러 전화 시스템 소프트웨어의 암호화 메카니즘(encryption mechanism) 또는 핸드셰이킹 메카니즘의 일부로서 하나 또는 두 개의 코드 모두를 사용할 수 있다. 만일 다른 메모리 장치가 셀룰러 전화 안에서 교체되었다면, 그 얼라인먼트(alignment)가 증명될 수 없고, 이 셀룰러 전화를 사용하여 셀룰러 네트워크에 액세스하는 것이 금지된다.

도1은 부정 방지 회로의 일실시예를 포함한 전자 시스템(100)을 도시한 도면이다. 이 전자 시스템(100)은 버스(104)에 연결된 중앙 처리 장치(Central Processor Unit: 이하, "CPU"라 칭함)(102)를 포함한다. 많은 응용 주문형 직접회로(Application-Specific Integrated Circuits: 이하, "ASIC"이라 칭함)(106-108)가 버스(104)에 연결되어, 특정 전자 시스템(100)의 동작을 가능하게 하지만, 본 실시예는 이에 한정되지 않는다. 메인 메모리(110)는 보조 메모리(112)와 함께 버스(104)에 연결된다. 보조 메모리(112)는 메인 메모리 어레이 공간(110)의 외부에 위치한 작은 메모리 어레이이다. 이로써, 보조 메모리(112)는 적어도 하나의 고유한 식별자 코드를 저장하는데 쓰여진다. 일실시예에서, 메인 메모리(110)는 플래시 메모리이지만, 본 실시예는 이에 한정되지 않는다. 또한, 보조 메모리(112)도 플래시 메모리일 수 있지만, 본 실시예는 이에 한정되지 않는다. 상기 전자 시스템(100)의 안전은 보조 메모리(112)를 메인 메모리(110)와 동일한 칩 상에 배치함으로써 최적화되지만, 본 실시예는 이에 한정되지 않는다. 일실시예에서, 전자 시스템(100)은 셀룰러 전화를 포함한다. 대안의 실시예에서, 전자 시스템(100)은 컴퓨터-기반(computer-based) 전자 시스템을 포함한다. 후술되는 상세한 설명에서는 전자 시스템(100)의 셀룰러 전화의 일례를 사용하겠지만, 본 실시예는 이에 한정되지 않는다.

도2는 플래시 메모리 장치(110)의 일실시예를 도시한 블록도이다. 명령 유저 인터페이스(Command User Interface: 이하, "CUI"라 칭함)(202)는 셀룰러 전화의 마이크로 프로세서 또는 마이크로 콘트롤러와 플래시 메모리 장치(110)의 내부 동작 사이에 인터페이스로 제공된다. 기록 상태 머신(Write State Machin: 이하 "WSM"으라 칭함)(204)은 검증을 포함한 프로그램 및 소거 동작에 대해 필요한 알고리즘 및 타이밍을 자동으로 수행한다. 따라서, 플래시 메모리 장치(110)는 셀룰러 전화의 CPU 또는 마이크로 콘트롤러를 통해 시스템 내부를 판독, 프로그램 및 소거한다. CUI(202)에서 제공된 명령은 유저가 메인 플래시 어레이(206) 및, 대안적으로 원타임 프로그램가능(One-Time Programmable: 이하, "OTP"라 칭함) 레지스터(210)에 액세스하는 것을 허가한다.

메모리 장치의 일실시예는 부정 사용을 방지하고, 시스템 설계의 안전을 증가시키기 위해 사용되는 보조 메모리 레지스터(210)를 포함한다. OTP 레지스터(210) 또는 보호 레지스터는 장치의 내부 위치에 저장된 128-비트 번호를 포함한다. 이 128-비트 보호 레지스터는 고유한 플래시 메모리 장치의 검증을 허가하며, 여기서 128-비트 번호는 셀룰러 전화와 같은 전자 장치에서 부정 방지를 위해 사용될 수 있지만, 본 발명은 이에 한정되지 않는다. 예를 들어, 보호 레지스터 안에 포함되는 번호는, 장치 교체를 방지하기 위하여, 상기 플래시 소자와 CPU, ASIC 및 신호 프로세서를 포함하는 그 외의 시스템 소자를 대비시키기 위해 사용될 수 있지만, 본 실시예는 이에 한정되지 않는다.

도3은 OTP 레지스터 또는 보호 레지스터의 일실시예의 메모리 맵(memory map)을 도시한 도면이다. 128-비트 보호 레지스터(300)는 두 개의 세그먼트(302- 304)를 포함하는데, 여기서, 각 세그먼트는 64비트를 포함하지만, 본 실시예는 이에 한정되지 않는다. 보호 레지스터(300)의 제1 세그먼트(302)는 제조 시점에서 메모리 장치 제조자에 의해 미리 프로그램된 고유한 부분의 번호를 포함한다. 그 번호는 제조된 각 장치에 대해 고유하다. 일실시예에서, 상기 미리 프로그램된 번호(64비트)는 패브 ID(fab IDentification)(8비트), 로트 ID(lot ID)(32비트), 웨이퍼 ID(8비트), 웨이퍼 위의 다이의 X위치(8비트) 및 웨이퍼 위의 다이의 Y위치(8비트)를 포함하는 어떤 조합을 이용하여 얻어질 수 있지만, 본 실시예는 이에 한정되지 않는다. 고유 식별 번호는 암호화될 수 있지만, 본 실시예는 이에 한정되지 않는다. 보호 레지스터(300)의 제1 세그먼트(302)는 로크(lock)되기 때문에, 일단 프로그램되면, 이 보호 레지스터(300)의 제1 세그먼트(302)의 컨텐츠(contents)는 변경이 불가능하다.

OTP 메모리 공간(300) 또는 보호 레지스터는 두 섹션에서 로크가능(lockable)하다. 보호 레지스터(300)의 제조자-프로그램가능 세그먼트, 즉 보호 레지스터(300)의 제1 세그먼트(302) 또는 제1 64비트(4워드 또는 8바이트)를 프로그래밍한 후, OTP 메모리 공간(300)의 제1 세그먼트는 추가의 로크 비트(312)를 기록함으로써 로크된다. OTP 메모리의 제1 세그먼트(302)는, 로크 어드레스 위치(320)에 "FFFF"(워드-와이드(word-wide)) 또는 "FE"(바이트-와이드(byte-wide)를 프로그램 하거나, 또는 기록하는 OTP 보호 프로그램 명령(OTP Protection Program command)을 이용하여 로크된다. 이 명령이 PR-LOCK 위치(312)의 비트 0을 0으로 프로그램 또는 설정하면, 첫 번째 64-비트(302)는 로크-아웃(lock out)된다. 이 로크아웃 비트(312-314)를 설정한 후, 보호 레지스터의 각 세그먼트에 저장된 값은 더 이상 변경이 허가되지 않는다. 로크된 보호 레지스터 세그먼트를 프로그램하려고 시도하면 상태 레지스터 에러(Status Register error)가 발생한다. 상기 보호 레지스터 로크아웃 상태는 다시 되돌릴 수 없지만, 본 실시예는 이에 한정되지 않는다.

보호 레지스터(304)의 제2 세그먼트는 유저에 의해 선택된 값으로 프로그램 가능한 세그먼트를 포함한다. 보호 레지스터 비트는 2-사이클 보호 프로그램(two-cycle Protection Program) 또는 OTP 프로그램(OTP Program) 명령을 이용하여 유저에 의해 프로그램된다. 64-비트 레지스터 값은 워드-와이드 부분에 대한 시간에서 16비트 및 바이트-와이드 부분에 대한 시간에서 8비트가 프로그램된다. 보호 레지스터(300)의 프로그래밍에서, 보호 프로그램 셋업(Protection Program Setup) 명령(C0H)은 첫 번째 사이클 동안 기록된다. 첫 번째 사이클은 OTP 프로그램 동작을 위해 CUI를 준비시킨다. 두 번째 사이클은 어드레스 및 데

18-4

[첨부그림 5]

아터 정보를 래치하고, OTP 프로그램 알고리즘을 OTP 레지스터에 수행하도록 기록 상태 머신을 초기화하는데, 여기서, 메모리 장치에 대한 다음의 기록은 OTP 레지스터의 특정한 위치를 프로그램한다. 도4는 보호 레지스터의 일실시예에 대하여 허용 가능한 워드-와이드 어드레싱을 도시한 도면이다. 도5는 보호 레지스터의 일실시예에 대하여 허용 가능한 바이트-와이드 어드레싱을 도시한 도면이다. 판독 어레이(Read Array) 명령은 프로그래밍 다음의 어레이 테이터를 판독하는데 사용된다. 정의된 보호 레지스터 어드레스 공간 외부의 보호 프로그램(Protection Program) 명령의 어드레싱을 시도하면 상태 레지스터 에러(Satus Register error)를 초래한다.

보호 레지스터의 유저-프로그램가능 세그먼트, 즉 보호 레지스터(300)의 제2 세그먼트(304) 또는 두 번째 64-비트를 프로그래밍한 후, OTP 메모리 공간(300)의 제2 세그먼트(304)는 추가의 로크 비트(314)를 기록함으로써 로크된다. OTP 메모리 공간(300)의 제2 세그먼트(304)는 "로크(LOCK)" 어드레스 위치(320)에 "FEED"(워드-와이드) 또는 "FD"(바이트-와이드)를 프로그램 또는 기록하는 보호 프로그램(Protection Program) 명령을 이용하여 로크된다. 이 명령이 "PR-LOCK" 위치(314)의 비트 1을 0으로 프로그램 또는 설정하면, 두 번째 64-비트(304)는 로크-아웃된다. 상기 로크아웃 비트(312-314)를 설정한 후에는, 보호 레지스터의 각 세그먼트에 저장된 값은 더 이상 변경이 허가되지 않는다. 보호 레지스터 세그먼트의 프로그래밍을 시도하면 상태 레지스터(Status Register) 에러를 초래한다. 보호 레지스터 로크아웃 상태는 역으로 되돌릴 수 없지만, 본 실시예는 이에 한정되지 않는다.

플래시 메모리 장치의 일실시예는 2개의 기록 모드와 4개의 판독 모드를 갖는다. 2개의 기록 모드는 프로그램(Program) 및 블록 소거(Block Erase)를 포함한다. 4개의 판독 모드는 어레이 판독(Read Array), 구성 판독(Read Configuration), 상태 판독(Read Status) 및 질의 판독(Read Query)을 포함한다. 적절한 판독 모드 명령은 해당 판독 모드로 들어가기 위해 CUI로 전송된다. 이에 따라, 보호 레지스터는 구성 판독(Read Conglguration) 모드에서 판독되고, 메모리 어레이에서 어드레싱할 수 없다.

구성 판독(Read Configuration) 모드는 제조자/장치 식별자 및 보호 레지스터의 컨텐츠, 즉 OTP 부정 방지 번호를 출력한다. 상기 장치는 구성 판독(Read Configuration) 명령(90H)를 CUI에 기록함으로써, 구성 판독(Read Configuration) 모드로 전환된다. 도6은 플래시 메모리 장치의 일실시예의 구성 판독(Read Configuration) 테이블을 도시한 도면이다. 상기 구성 판독(Read Configuration) 테이블은, 판독 사이클 동안 플래시 메모리 장치에 나타난 어드레스로부터 구성 판독 모드에서 검색된 특정한 정보의 테이블이다. 구성 판독 모드에서 도4 및 도5의 어드레스에서의 판독 사이클은 보호 레지스터에서 값을 검색한다.

도7은 전자 시스템 제어 방법의 일실시예를 도시한 순서도이다. 단계(702)에서 동작이 시작되는데, 여기서, 적어도 하나의 고유 코드가 전자 시스템의 보조 메모리 안에 프로그램된다. 보조 메모리는 메인 메모리 어레이 공간의 외부에 위치한 영구적 로크가능 메모리(permanently lockable memory)이다. 이 보조 메모리는 구성 메모리 공간 안에 위치할 수 있지만, 본 실시예는 이에 한정되지 않는다. 단계(704)에서, 고유 코드는 적어도 하나의 소자 코드와 비교된다. 전자 시스템의 사용은 상기 고유 코드와 소자 코드 사이에 사전 정의된 관계를 바탕으로 제어된다. 단계(706)에서, 상기 사전 정의된 관계가 만족되는지의 여부에 대한 판정이 이루어진다. 일실시예에서, 상기 사전 정의된 관계는 상기 고유 코드와 소자 코드 사이의 부합(match)이지만, 본 실시예는 이에 한정되지 않는다. 만일, 이 사전 정의된 관계가 만족된다면, 단계(708)에서 전자 시스템에 대한 사용 또는 액세스가 허가된다. 만일, 상기 사전 정의된 관계가 만족되지 않는다면, 단계(710)에서 전자 시스템의 사용이 허가되지 않는다.

이 전자 시스템은 셀룰러 전화, 내장형 시스템(embedded system) 및 셋탑 박스(set-top box)를 포함하지만, 본 실시예는 이에 한정되지 않는다. 일실시예의 메인 메모리는 플래시 메모리이다. 일실시예의 보조 메모리는 플래시 메모리이다. 일실시예에서, 상기 메인 메모리 및 보조 메모리는 동일한 집적 회로 또는 칩 상에 위치하지만, 본 실시예는 이에 한정되지 않는다. 대안의 실시예에서, 보조 메모리는 시리얼 포트(serial port) 및 입/출력 포트(I/O port)를 사용하여 액세스할 수 있다.

일실시예에서, 소자 코드는 전자 시스템의 적어도 하나의 소자의 원타임 프로그램가능 메모리(one-time programmable memory) 안에 설정 또는 저장되는 반면, 고유 코드는 보조 메모리의 세그먼트에 저장된다. 상기 전자 시스템의 소자는 메모리, 마이크로 콘트롤러, ASIC, CPU, 신호 프로세서 및 SIM 카드를 포함할 수 있지만, 본 실시예는 이에 한정되지 않는다.

대안의 실시예에서, 고유 코드는 보조 메모리의 제1 세그먼트에 저장되고, 소자 코드는 보조 메모리의 제2 세그먼트에 저장되지만, 본 실시예는 이에 한정되지 않는다. 이 대안적 실시예에서, 고유 코드는 식별 코드를 암호화하도록 사용된다. 상기 식별 코드는 전자 시스템의 메인 메모리에 저장된 적어도 하나의 비트를 포함한다. 또한, 상기 식별 코드 또는 번호는 전자 시스템의 시스템 소프트웨어 안에 내재된 식별 코드를 포함한다. 이 암호화된 식별 코드는 보조 메모리에 저장된 소자 코드와 비교된다. 상기 암호화된 식별 코드와 소자 코드가 부합되지 않을 경우, 이 전자 시스템에 대한 사용 및 액세스가 디스에이블된다.

다른 대안적 실시예에서는, 소자 코드가 식별 코드를 암호화하는데 사용된다. 암호화된 식별 코드는 보조 메모리에 저장된 고유 코드와 비교된다. 상기 암호화된 식별 코드와 고유 코드가 부합되지 않을 경우, 이 전자 시스템에 대한 사용 및 액세스는 디스에이블된다.

다른 대안적 실시예에서, 소자 코드는 고유 코드를 이용하여 암호화된다. 이 암호화된 소자 코드와 전자 시스템의 시스템 소프트웨어의 메인 메모리에 저장된 적어도 하나의 코드가 부합되지 않는 경우, 이 전자 시스템에 대한 사용 및 액세스는 디스에이블된다.

도8은 부정 방지 방법의 일실시예를 도시한 순서도이다. 단계(802)에서 동작이 시작되는데, 이때, 고유 코드가 셀룰러 전화 보조 메모리의 보호 레지스터 안에 프로그램된다. 여기서 이미 논의된 바와 같이, 상기 보조 메모리는 영구적 로크가능 메모리 또는 원타임 프로그램가능 메모리이다. 이전에 논의된 바와 같이, 고유 코드는 메모리 장치 제조자에 의해 보호 레지스터의 첫 번째 64-비트 안에 프로그램되고, 로크 비트가 설정되는데, 여기서 고유 코드의 수정은 금지된다. 셀룰러 전화 OEM에 의해 이 메모리 장치가 수신되자마자, 제조자에 의해 설정됨에 따라 고유 코드는 셀룰러 전화를 부정 복제로부터 보호하기 위해 사용될 수 있다. 또한, 보호 레지스터의 두 번째 64-비트 세그먼트가 제공되는데, 여기에 셀룰러 전화 OEM

18-5

[첨부그림 6]

에 의해 고유 코드가 프로그램될 수 있다. 셀룰러 전화 OEM에 의해 고유 코드가 프로그램된 후 로크 비트가 설정되는데, 여기서 상기 고유 코드는 수정이 금지된다. 상기 프로그램된 코드 중 하나 또는 양쪽 모두는 셀룰러 전화 OEM에 의해 부정 방지 구조에서 사용될 수 있다.

단계(804)에서, 고유 코드는 소자 코드와 비교된다. 상기 고유 코드와 소자 코드 사이에 사전 정의된 관계를 바탕으로 셀룰러 전화의 사용이 제어된다. 단계(806)에서, 상기 사전 정의된 관계가 만족되는지의 여부에 대한 판정이 이루어진다. 일실시예에서, 상기 사전 정의된 관계는 소프트웨어 질의(software query)에 의해 검증되는 고유 코드와 소자 코드 간의 부합이지만, 본 실시예는 이에 한정되지 않는다. 만일, 상기 사전 정의된 관계가 만족된다면, 단계(808)에서 셀룰러 전화의 사용이 허가된다. 만일, 상기 사전 정의된 관계가 만족되지 않는다면, 단계(810)에서 셀룰러 전화의 사용이 허가되지 않는다. 대안의 실시예에서는, 상기 사전 정의된 관계가 만족되지 않는 경우, 셀룰러 전화의 제한된 활성화(activation)가 추적 목적을 위해 허용될 수 있지만, 본 실시예는 이에 한정되지 않는다. 대안의 실시예에서, 상기 사전 정의된 관계가 만족되지 않는 경우, 셀룰러 서비스 제공자에 접속한 유저에게 알리기 위하여 메시지가 디스플레이될 수 있다.

고유 코드와 소자 코드 사이의 사전 정의된 관계는 이 코드들 간의 부합일 수 있지만, 본 실시예는 이에 한정되지 않는다. 대안의 실시예에서, 셀룰러 전화의 사용은 고유 코드를 암호화(encrypt) 또는 복호화(decrypt)하는 소자 코드를 이용하여 제어될 수 있다. 다른 대안적 실시예에서는, 소자 코드를 암호화 또는 복호화 하는 고유 코드를 이용하여 셀룰러 전화의 사용이 제어될 수 있다. 추가적인 대안의 실시예에서는, 고유 코드 및 소자 코드를 셀룰러 전화 시스템 소프트웨어에 대한 암호화 검증 키(encryption validation key)로 사용하여, 셀룰러 전화의 사용이 제어될 수 있다.

일실시예에서, 소자 코드는 셀룰러 전화의 영구적 로크가능 메모리 또는 적어도 하나의 구성요소의 원타임 프로그램가능 메모리 안에 설정 또는 저장되는 반면, 고유 코드는 보조 메모리의 세그먼트 안에 저장된다. 소자 코드는 셀룰러 전화 OEM 또는 셀룰러 서비스 제공자에 의해 프로그램될 수 있다. 대안적으로, 셀룰러 전화 OEM은 셀룰러 서비스 제공자에 의해 제공된 바와 같이 소자 코드를 프로그램할 수 있다. 이러한 방식에서, 셀룰러 전화의 다수의 소자가 함께 링크됨으로써, 예를 들어, 플래시 메모리와 같이 링크된 소자가 제거되어 다른 소자로 교체된 경우, 셀룰러 전화의 사용을 금지할 수 있다. 셀룰러 전화의 소자는 메모리, 마이크로 콘트롤러, ASIC, CPU 및 신호 프로세서를 포함할 수 있지만, 본 실시예는 이에 한정되지 않는다. GSM 셀룰러 전화는, 이에 한정되지 않지만, 요금 계산 데이터, 폰북(phone book) 및 우선 처리 통화(call handing preference)를 포함한 유저의 개인적인 정보를 나르는 포터블 SIM 카드(portable Subscriber Identification Module card)를 사용한다. 이 GSM 시스템에서, SIM 카드가 다른 전화에서 사용될 수 있기 때문에, 소자 코드는 셀룰러 전화 인프라스트럭쳐(infrastructure)의 소자 안에 설정될 수 있는데, 여기서 상기 인프라스트럭쳐는 SIM 카드 안에 내재된 유저 프로파일(user profile)을 포함한다.

대안적 실시예에서, 고유 코드는 보조 메모리의 제1 세그먼트에 저장되고, 소자 코드는 보조 메모리의 제2 세그먼트네 저장되지만, 본 실시예는 이에 한정되지 않는다. 이러한 대안적 실시예에서, 고유 코드는 식별 번호를 암호화하는데 사용된다. 상기 식별 번호는 ESN, IMEI 및 셀룰러 전화에 의해 셀룰러 기지국으로부터 수신된 신호에서 셀룰러 서비스 제공자에 의해 제공된 번호가 포함된다. 그리고, 식별 번호는 전자 시스템의 메인 메모리 안에 저장된 번호를 포함할 수 있다. 또한, 식별 번호는 전자 시스템의 시스템 소프트웨어 안에 내재된 식별자 번호를 포함할 수 있다. 암호화된 식별 번호는 보조 메모리에 저장된 소자 코드와 비교된다. 상기 암호화된 식별 번호와 소자 코드가 부합되는 경우, 셀룰러 전화의 사용이 허가된다.

다른 대안적 실시예에서, 셀룰러 전화 서비스 제공자는 셀룰러 전화로부터 고유 코드를 판독하여 암호화된 방식으로 GSM SIM 카드 안에 고유 코드를 프로그램할 수 있다. 셀룰러 전화의 활성화가 시도되면, 셀룰러 전화 소프트웨어는 고유 코드와 상기 프로그램된 코드를 비교할 것이다. 대안적으로, GSM SIM 카드의 메모리 안에 내재된 코드는 영구적 로크가능 메모리 안에 프로그램될 수 있으며, 여기서 셀룰러 전화 소프트웨어는 상기 두 코드를 비교할 것이다.

일실시예에서, 셀룰러 전화의 메인 메모리에 대한 액세스를 금지함으로써, 셀룰러 전화의 사용이 방지되지만, 본 실시예는 이에 한정되지 않는다. 대안적 실시예에서는, 셀룰러 전화의 시스템 소프트웨어를 복호화하는 고유 코드 및 소자 코드를 이용하여 셀룰러 전화의 사용이 허가된다. 다른 대안적 실시예에서는, 암호화 키와 함께 고유 코드를 이용하여 셀룰러 전화의 사용이 허가된다.

상기 상세한 설명에서는 플래시 EPROM을 이용하는 실시예를 기술하였지만, 본 발명은 어떠한 비휘발성 기록가능 메모리와 함께 사용될 수 있다. 본 발명이 특정 실시예를 참조하여 설명되었지만, 첨부된 청구항에서 설명된 바와 같이, 본 발명의 보다 넓은 사상 및 범위에서 벗어나지 않는 한, 다양한 수정 및 변경이 가능하다는 것은 명백한 사실이다. 따라서, 본 명세서 및 도면은 제한적 관점이라기 보다는 하나의 예시로서 간주되어야 한다.

(57) 청구의 범위

청구항 1

전자 시스템의 사용을 제어하기 위한 방법에 있어서,

상기 전자 시스템의 보조 메모리 안에 적어도 하나의 고유 코드를 프로그래밍하는 단계 - 여기서, 상기 보조 메모리는 로크가능 메모리임 -;

상기 적어도 하나의 고유 코드와 적어도 하나의 소자 코드를 비교하는 단계; 및

상기 적어도 하나의 고유 코드와 상기 적어도 하나의 소자 코드 사이에 사전 정의된 관계를 바탕으로 상기 전자 시스템의 사용을 제어하는 단계

를 포함하는 방법.

18-6

[첨부그림 7]

청구항 2

제1항에 있어서,

상기 적어도 하나의 고유 코드와 상기 적어도 하나의 소자 코드가 부합되지 않는 경우, 상기 전자 시스템의 사용을 디스에이블 시키고, 상기 전자 시스템에 대한 액세스를 디스에이블 시키는 단계

를 더 포함하는 방법.

청구항 3

제1항에 있어서,

상기 적어도 하나의 고유 코드를 이용하여 식별 코드를 암호화하는 단계; 및

상기 암호화된 식별 코드와 상기 적어도 하나의 소자 코드가 부합되지 않는 경우, 상기 전자 시스템의 사용을 디스에이블 시키고, 상기 전자 시스템에 대한 액세스를 디스에이블 시키는 단계

를 더 포함하는 방법.

청구항 4

제3항에 있어서,

상기 식별 코드는 상기 전자 시스템의 메인 메모리 안에 저장된 적어도 하나의 비트를 포함하는

방법.

청구항 5

제3항에 있어서,

상기 식별 코드는 상기 전자 시스템의 시스템 소프트웨어 안에 내재된 적어도 하나의 비트를 포함하는

방법.

청구항 6

제1항에 있어서,

상기 적어도 하나의 고유 코드를 이용하여 상기 적어도 하나의 소자 코드를 암호화하는 단계; 및

상기 적어도 하나의 소자 코드와 상기 전자 시스템의 메인 메모리 안에 저장된 적어도 하나의 코드가 부합되지 않는 경우, 상기 전자 시스템의 사용을 디스에이블 시키고, 상기 전자 시스템에 대한 액세스를 디스에이블 시키는 단계

를 더 포함하는 방법.

청구항 7

제3항에 있어서,

상기 적어도 하나의 고유 코드는 상기 보조 메모리의 제1 세그먼트 안에 저장되고, 상기 적어도 하나의 소자 코드는 상기 보조 메모리의 제2 세그먼트 안에 저장되는

방법.

청구항 8

제1항에 있어서,

상기 적어도 하나의 소자 코드를 상기 전자 시스템의 적어도 하나의 소자의 원타임 프로그램가능 메모리 안에 설정하는 단계

를 더 포함하는 방법.

청구항 9

제8항에 있어서,

상기 적어도 하나의 소자는 마이크로 콘트롤러, 응용 주문형 집적회로(ASIC), 중앙 처리 장치(CPU), 신호 프로세서 및 가입자 식별 모듈(SIM) 카드를 포함하는

방법.

청구항 10

제1항에 있어서,

상기 전자 시스템은 셀룰러 전화를 포함하는

방법.

청구항 11

18-7

[첨부그림 8]

제1항에 있어서,

상기 메인 메모리는 플래시 메모리인

방법.

청구항 12

제1항에 있어서,

상기 메인 메모리 및 상기 보조 메모리는 동일한 칩 상에 위치하는

방법.

청구항 13

제1항에 있어서,

상기 로크가능 메모리는 원타임 프로그램가능 메모리인

방법.

청구항 14

제1항에 있어서,

상기 보조 메모리는 메인 메모리 어레이 공간의 외부에 위치하는

방법.

청구항 15

제2항에 있어서,

상기 전자 시스템은 내장형 시스템인

방법.

청구항 16

제2항에 있어서,

상기 전자 시스템은 셋탑 박스인

방법.

청구항 17

제1항에 있어서,

상기 보조 메모리는 영구적으로 로크가능한

방법.

청구항 18

셀룰러 전화의 사용을 제어하기 위한 방법에 있어서,

상기 셀룰러 전화의 보조 메모리 안에 적어도 하나의 고유 코드를 프로그래밍하는 단계 - 여기서, 상기 보조 메모리는 로크가능 메모리임 -;

상기 적어도 하나의 고유 코드와 적어도 하나의 소자 코드를 비교하는 단계; 및

상기 적어도 하나의 고유 코드와 상기 적어도 하나의 소자 코드 간에 사전 정의된 관계를 바탕으로 상기 셀룰러 전화의 사용을 제어하는 단계

를 포함하는 방법.

청구항 19

제18항에 있어서,

상기 적어도 하나의 고유 코드를 이용하여 식별 코드를 암호화하는 단계; 및

상기 암호화된 코드와 상기 적어도 하나의 소자 코드가 부합되는 경우, 전화 통화가 이루어지도록 허가하는 단계

를 더 포함하는 방법.

청구항 20

제19항에 있어서,

상기 식별 코드는 장치 일련 번호(ESN) 및 국제 이동 장치 식별자(IMEI)를 포함하는

방법.

18-8

[첨부그림 9]

청구항 21

제19항에 있어서,

상기 식별 코드는 상기 셀룰러 전화에 의해 수신된 신호에서 상기 셀룰러 서비스 제공자에 의해 제공된 적어도 하나의 비트를 포함하는

방법.

청구항 22

제18항에 있어서,

상기 적어도 하나의 고유 코드는 상기 보조 메모리의 제1 세그먼트 안에 저장되고, 상기 적어도 하나의 소자 코드는 상기 보조 메모리의 제2 세그먼트 안에 저장되는

방법.

청구항 23

제18항에 있어서,

상기 적어도 하나의 고유 코드와 상기 적어도 하나의 소자 코드가 부합되는 경우 전화 통화가 이루어지도록 허가하는 단계

를 더 포함하는 방법.

청구항 24

제18항에 있어서,

상기 적어도 하나의 소자 코드를 상기 셀룰러 전화의 적어도 하나의 소자의 영구적 로크가능 메모리 안에 설정하는 단계

를 더 포함하는 방법.

청구항 25

제24항에 있어서,

상기 적어도 하나의 소자는 마이크로 콘트롤러, ASIC, CPU 및 신호 프로세서를 포함하는

방법.

청구항 26

제25항에 있어서,

상기 적어도 하나의 소자 코드를 상기 셀룰러 전화 인프라스트럭쳐의 적어도 하나의 소자 안에 설정하는

방법.

청구항 27

제26항에 있어서,

상기 셀룰러 전화 인프라스트럭쳐의 상기 적어도 하나의 소자는 유저 프로파일을 포함한 SIM 카드를 포함하는

방법.

청구항 28

제18항에 있어서,

상기 사용 제어 단계는 상기 적어도 하나의 고유 코드 및 상기 적어도 하나의 소자 코드를 상기 셀룰러 전화의 시스템 소프트웨어에 대한 암호화 검증 키로 사용하는 단계를 포함하는

방법.

청구항 29

제18항에 있어서,

상기 메인 메모리는 플래시 메모리이고,

여기서, 상기 메인 메모리 및 상기 보조 메모리는 동일한 칩 상에 위치하는

방법.

청구항 30

제18항에 있어서,

상기 프로그래밍 단계는 상기 보조 메모리의 제1 레지스터 안에 고유 코드를 프로그래밍하는 단계를 포함

18-9

[첨부그림 10]

하고,

여기서, 상기 프로그래밍 단계는 상기 메인 메모리의 제조자에 의해 수행되고, 상기 제1 레지스터는 64-비트 레지스터인

방법.

청구항 31

제30항에 있어서,

제1 로크 레지스터의 적어도 하나의 로크 비트를 이용하여 상기 제1 레지스터 안에 상기 고유 코드를 로킹함으로써, 상기 고유 코드의 수정을 방지하는 단계

를 더 포함하는 방법.

청구항 32

제18항에 있어서,

상기 프로그래밍 단계는 상기 보조 메모리의 제2 레지스터 안에 고유 코드를 프로그래밍하는 단계를 포함하고,

여기서, 상기 제2 레지스터는 64-비트 레지스터인

방법.

청구항 33

제32항에 있어서,

제2 로크 레지스터의 적어도 하나의 로크 비트를 이용하여 상기 제2 로크 레지스터 안에 상기 고유 코드를 로킹함으로써, 상기 고유 코드의 수정을 방지하는 단계

를 더 포함하는 방법.

청구항 34

제18항에 있어서,

상기 보조 메모리는 메인 메모리 어레이 공간의 외부에 위치하고,

여기서, 상기 보조 메모리는 영구적으로 로크가능한

방법.

청구항 35

셀룰러 전화의 사용을 제어하기 위한 장치에 있어서,

적어도 하나의 고유 코드를 포함하는 보조 메모리 - 상기 보조 메모리는 로크가능함 -; 및

상기 보조 메모리에 연결되며, 적어도 하나의 소자 코드를 검색하여 상기 적어도 하나의 고유 코드와 상기 적어도 하나의 소자 코드를 비교하도록 구성되고, 상기 적어도 하나의 고유 코드가 상기 적어도 하나의 소자 코드와의 사전 정의된 관계를 만족시키는 경우, 전화 통화가 이루어지도록 허가하는 부정 방지 회로

를 포함하는 장치.

청구항 36

제35항에 있어서,

상기 상기 적어도 하나의 고유 코드를 이용하여 식별 코드가 암호화되고,

여기서, 상기 암호화된 식별 코드와 상기 적어도 하나의 소자 코드가 부합되는 경우 전화 통화가 이루어질 수 있는

장치.

청구항 37

제35항에 있어서,

상기 적어도 하나의 고유 코드는 상기 보조 메모리의 제1 세그먼트 안에 저장되도, 상기 적어도 하나의 소자 코드는 상기 보조 메모리의 제2 세그먼트 안에 저장되는

장치.

청구항 38

제35항에 있어서,

상기 적어도 하나의 고유 코드와 상기 적어도 하나의 소자 코드가 부합되는 경우 전화 통화가 이루어질 수 있는

18-10

[첨부그림 11]

장치.

청구항 39

제35항에 있어서,

상기 셀룰러 전화의 적어도 하나의 소자로부터 상기 적어도 하나의 소자 코드가 검색되고,

여기서, 상기 적어도 하나의 소자는 마이크로 콘트롤러, ASIC, CPU, SIM 카드 및 신호 프로세서를 포함하는

장치.

청구항 40

제35항에 있어서,

상기 보조 메모리는 메인 메모리 어레이 공간의 외부에 위치하고, 영구적 로크가능 메모리인

장치.

청구항 41

셀룰러 전화에 있어서,

버스에 연결된 CPU 및 적어도 하나의 ASIC;

버스에 연결된 메인 메모리 및 보조 메모리 - 여기서, 상기 보조 메모리는 적어도 하나의 고유 코드를 포함하고, 메인 메모리 어레이 공간의 외부에 위치하며, 영구적으로 로크가능함 -; 및

상기 보조 메모리에 연결되며, 적어도 하나의 소자 코드를 검색하여 상기 적어도 하나의 고유 코드와 상기 적어도 하나의 소자 코드를 비교함으로써 상기 셀룰러 전화의 사용을 제어하도록 구성되고, 상기 적어도 하나의 고유 코드가 상기 적어도 하나의 소자 코드와의 사전 정의된 관계를 만족시키는 경우, 전화 통화가 이루어지도록 허가하는 부정 방지 회로

를 포함하는 셀룰러 전화.

청구항 42

제41항에 있어서,

상기 적어도 하나의 고유 코드를 이용하여 식별 코드가 암호화되고,

여기서, 상기 암호화된 식별 코드와 상기 적어도 하나의 소자 코드가 부합되는 경우 전화 통화가 이루어질 수 있는

셀룰러 전화.

청구항 43

제42항에 있어서,

상기 식별 코드는 상기 셀룰러 전화의 메인 메모리 안에 저장된 적어도 하나의 비트를 포함하고,

여기서, 상기 적어도 하나의 비트는 셀룰러 전화에 의해 수신된 신호에서 셀룰러 서비스 제공자에 의해 제공되고, 상기 셀룰러 전화의 시스템 소프트웨어 안에 내재되는

셀룰러 전화.

청구항 44

제43항에 있어서,

상기 적어도 하나의 고유 코드는 상기 보조 메모리의 제1 세그먼트 안에 저장되고, 상기 적어도 하나의 소자 코드는 상기 보조 메모리의 제2 세그먼트 안에 저장되며,

여기서, 상기 메인 메모리 및 상기 보조 메모리는 동일한 칩 상에 위치하는

셀룰러 전화.

청구항 45

프로세싱 시스템에서 실행되는 경우, 상기 시스템이 셀룰러 전화의 사용을 제어하기 위한 단계를 수행하도록 하는 실행가능한 명령어를 포함하는 컴퓨터-판독가능 매체에 있어서,

상기 셀룰러 전화의 사용을 제어하는 단계는,

적어도 하나의 고유 코드를 셀룰러 전화의 보조 메모리 안에 프로그래밍하는 단계 - 여기서, 상기 보조 메모리는 로크가능 메모리임 -;

상기 적어도 하나의 고유 코드와 적어도 하나의 소자 코드를 비교하는 단계; 및

상기 적어도 하나의 고유 코드와 상기 적어도 하나의 소자 코드 간에 사전 정의된 관계를 바탕으로 상기 셀룰러 전화의 사용을 제어하는 단계를 포함하는

18-11

[첨부그림 12]

컴퓨터-판독가능 매체.

청구항 46

제45항에 있어서,

상기 실행가능한 명령어는 또한 상기 적어도 하나의 고유 코드와 상기 적어도 하나의 소자 코드가 부합되는 경우, 상기 시스템이 전화 통화가 이루어지도록 허가하는 단계를 수행하도록 하는

컴퓨터-판독가능 매체.

청구항 47

제45항에 있어서,

상기 적어도 하나의 소자 코드는 상기 셀룰러 전화의 적어도 하나의 소자의 원타임 프로그램가능 메모리에 설정되고,

여기서, 상기 적어도 하나의 소자는 마이크로 콘트롤러, ASIC 및 CPU를 포함하는

컴퓨터-판독가능 매체.

청구항 48

제45항에 있어서,

상기 메인 메모리는 플래시 메모리이고,

여기서, 상기 메인 메모리 및 상기 보조 메모리는 동일한 칩 상에 위치하는

컴퓨터-판독가능 매체.

청구항 49

제45항에 있어서,

상기 보조 메모리는 메인 메모리 어레이 공간의 외부에 위치하고, 영구적 로크가능 메모리인

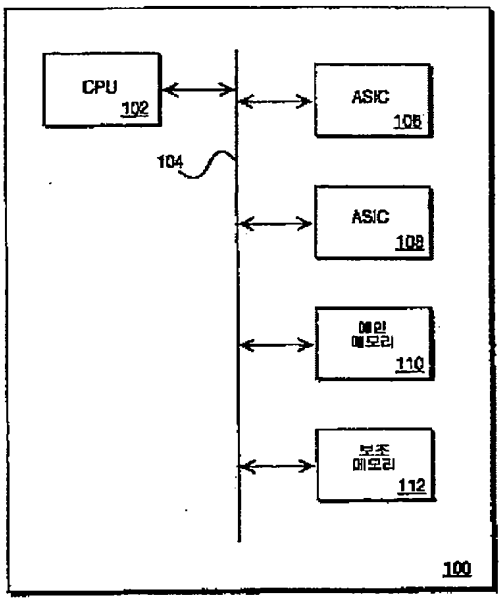
컴퓨터-판독가능 매체.

도면

18-12

[첨부그림 13]

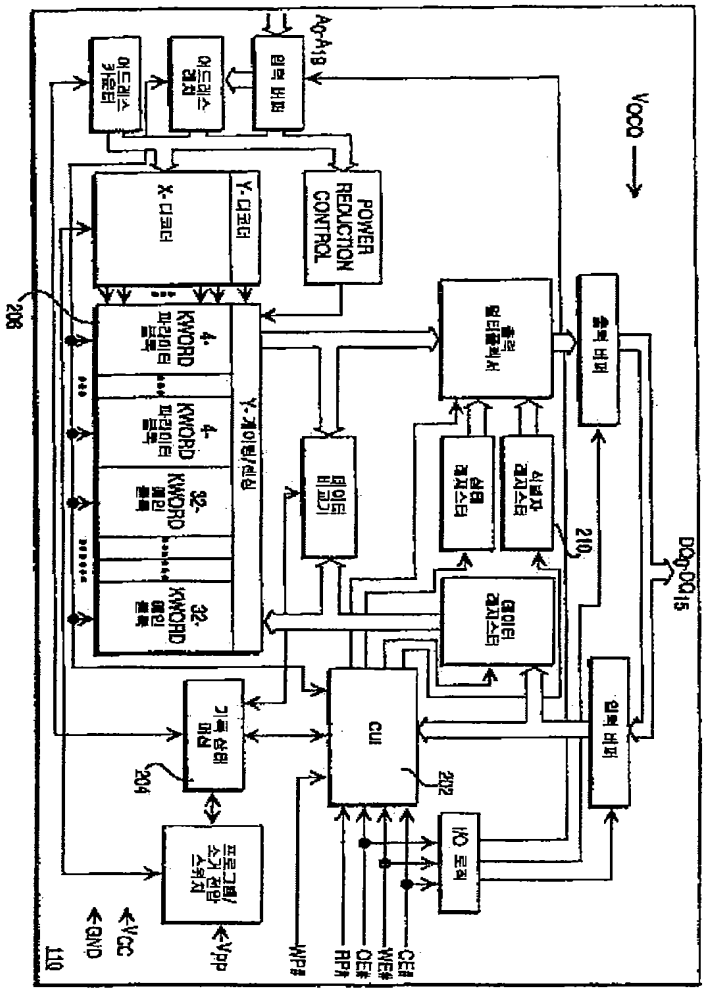
도면1



18-13

[첨부그림 14]

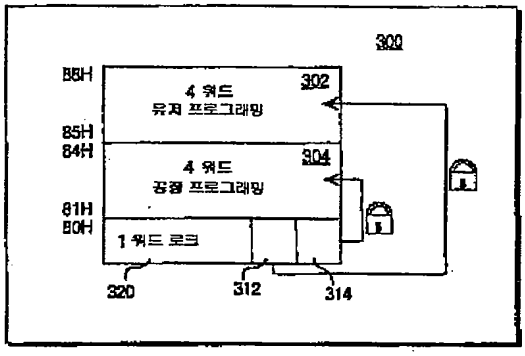
도면2



18-14

[첨부그림 15]

도면3



도면4

워드-와이드 보호 레지스터 어드레싱

워드	A7	A6	A5	A4	A3	A2	A1	A0	로크	사용
0	1	0	0	0	0	0	0	1	공장	유저모두
1	1	0	0	0	0	0	1	0	로킹	공장
2	1	0	0	0	0	1	0	0	로킹	공장
3	1	0	0	0	0	1	0	1	로킹	공장
4	1	0	0	0	0	1	1	0	로킹	유저
5	1	0	0	0	0	1	1	1	로킹	유저
6	1	0	0	0	1	0	0	0	로킹	유저
7	1	0	0	0	1	0	0	1	로킹	유저

18-15

[첨부그림 16]

도면5

바이트-와이드 보호 레지스터 어드레싱

바이트	사용	A11	A7	A6	A5	A4	A3	A2	A1	A0
로크	양쪽모두	0	1	0	0	0	0	0	0	0
0	공장	1	1	0	0	0	0	0	0	0
1	공장	0	1	0	0	0	0	0	0	1
2	공장	1	1	0	0	0	0	0	0	1
3	공장	0	1	0	0	0	0	0	1	0
4	공장	1	1	0	0	0	0	0	1	0
5	공장	0	1	0	0	0	0	0	1	1
6	공장	1	1	0	0	0	0	0	1	1
7	공장	0	1	0	0	0	0	1	0	0
8	유저	1	1	0	0	0	0	1	0	0
9	유저	0	1	0	0	0	0	1	0	1
10	유저	1	1	0	0	0	0	1	0	1
11	유저	0	1	0	0	0	0	1	1	0
12	유저	1	1	0	0	0	0	1	1	0
13	유저	0	1	0	0	0	0	1	1	1
14	유저	1	1	0	0	0	0	1	1	1
15	유저	0	1	0	0	0	1	0	0	0

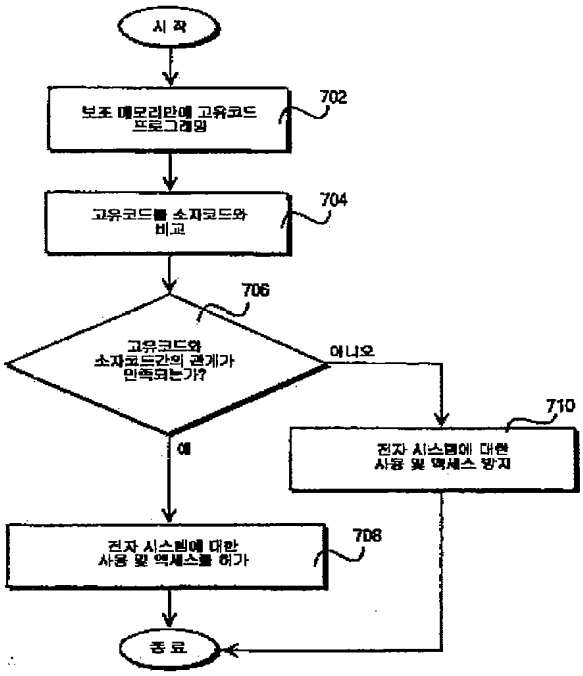
도면6

항목	어드레스	데이터
제조자 코드 (x16)	00000	0089
제조자 코드 (x8)	00000	89
장치 ID	00001	ID
블록 로크 구성	XX002	LOCK
● 블록이 로크되지 않음		DQ_0=0
● 블록이 로크됨		DQ_0=1
● 블록이 로크다운됨		DQ_1=1
보호 레지스터 로크	80	PR-LK
보호 레지스터 (x16)	81-88	PR
보호 레지스터 (x8)		PR

18-16

[첨부그림 17]

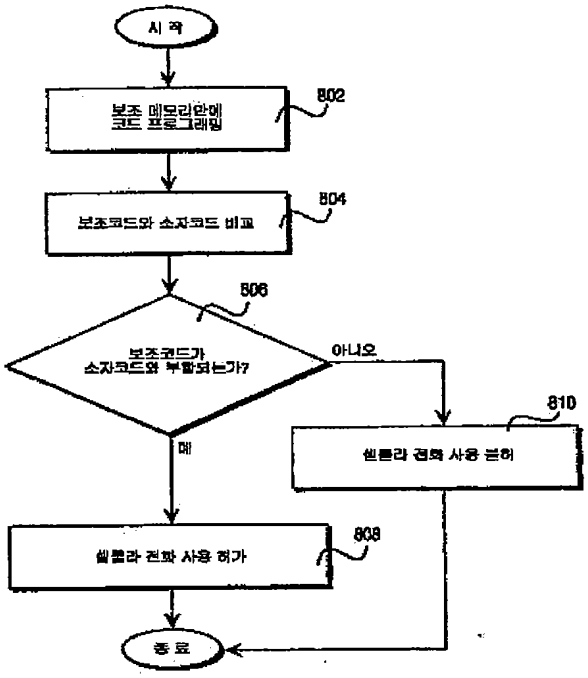
도면7



18-17

[첨부그림 18]

도면8



18-18